徐彥旻 b03901027

R. Anderson, “Why cryptosystems fail,” in Proceedings of the 1st ACM Conference on Computer and Communications Security, 1993.

摘要

本篇主要在提出資安領域專注的焦點與實際發生的情況有很大的落差，經常發生的問題肇因於組織與人力因素，但卻長期被忽視，而無法建立完整的資安維護體系。
在以 ATM 做金融交易的年代，這樣的問題就造成了相當的金融損失與大量的爭議案件以及訴訟。而在現在線上服務蓬勃發展的現在，資訊安全的結構性隱憂也不曾消失。
作者將這樣的現象歸因於歷史因素、現行商業模型、以及資安人員難以在企業中找到定位等因素，並提出從元件導向到考量組織與人力的整題「典範轉移」作為未來可能的方向。

段落大意
一、與航空安全相較，資訊安全的事件能見度很低，更缺乏圈內的制度化學習機制，導致整個領域的人難以從錯誤中學習。這一部分肇因於密碼系統的使用者通常是政府單位，以及冷戰的歷史因素。

二、比較了不同國家對於銀行的法律規定，以及衍生而出的爭議案。提到了分析自動櫃員機的緣由(在 1992 年的集體訴訟中提供專業意見)，為第三段的討論鋪陳。

三、 ATM 詐騙如何發生
* (1) 此段提供了許多簡單的攻擊案例，從卡片分配的方式、銀行上級想要壓低成本、開發測試時的設計，到 PIN 碼、磁條設計不良、ATM 離線工作等，在在使得櫃檯人員、跟櫃員機相關的非領域專業人士、以及意圖偽造的人能夠這個攻擊系統。
* (2) 銀行可能沒有更新設備，或不懂什麼是好的設備、甚或是買了好的設備亂裝，就算都裝好了也有被密碼分析破解的可能。銀行家不願承認失誤、安於現狀，看來很難有清晰合理的策略出現。
* (3) 目前的商業模式不合理，安全設備的使用者沒有能力正確的使用設備，應

該出現解決方案與人員訓練的提供者，並設計能在系統層級上能被專業的計算機人員整合管理、維持運作的產品。

四、 資訊安全領域的軍事歷史導致在發展 ATM 時的風險模型錯誤；而資安人員難以融入企業組織中，以及資安設備的可及性高，造成使用者的素質低落並且過度自信。

五、 提出資訊安全需要典範轉移，從單一設備層面轉向，全面地去考量組織與組織中的人力。因此，現行的「設備認證」也應該要能夠改變，需要重新改寫，考量系統因素與人力。

優點

以詳盡的自動櫃員機的案例讓讀者能夠理解資訊安全在實際的狀況中各種失敗、失效的可能狀況，即使是入門者仍能夠理解作者想要傳達的結構性問題，並且有提出他所想的解決方法——考量到設備使用環境（包含組織與人）的典範轉移，作為未來可能的方向。

缺點

在末段提出的兩種哲學與比喻的競爭讓人摸不著頭緒，也許是因為是十年前的論文，跟現在的時代有落差，不好體會。

反思

在他提出的，使用者素質低落的現象，現今仍然存在，舉例來說，2016 台灣駭客年會就有整理一系列令人啼笑皆非的資安相關的報導。此外在戲劇影視當中對於資安領域的想像仍然是很貧乏的，再加上之前的第一銀行自動櫃員機盜領案，至少在台灣有許多的現象是與十年前相同的。